AFFIDAVIT OF BORDER PATROL AGENT ADRIAN GOMEZ

Your affiant, Adrian Gomez, Border Patrol Agent of the United States Border Patrol, being duly sworn, does depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Border Patrol Agent with the United States Border Patrol ("USBP") permanently assigned to the Sonoita Border Patrol Station in Sonoita, Arizona and serving my second detail to Tucson Sector Prosecutions Unit in Tucson, Arizona. I have been an agent with the USBP since May 8, 2008. I completed the USBP Academy on March 19, 2009, where I received instruction in constitutional law, immigration law, criminal law, and federal and civil statutes. I have also received instruction in the detection, interdiction, and arrest of narcotics smugglers, alien smugglers, and aliens illegally present in the United States.

2. As a Border Patrol Agent, I work routine field agent duties patrolling the Sonoita Area of Operations ("AOR"). I been involved in many apprehensions of undocumented aliens, alien smugglers, narcotic traffickers and facilitators. I have processed and presented many cases for criminal prosecution and administrative proceedings.

3. I have been previously detailed to the Sonoita Station Intel Unit, as well as two detail iterations to the Alien Smuggling Identification and Deterrence Unit at the Sonoita Border Patrol station. I was also previously detailed to the San Rafael Valley Project where I was assigned to Homeland Security Investigations office in Rio Rico, Arizona, as Task Force Officer. While on detail, I planned operations, conducted surveillance, gathered intelligence,

created target folders, worked targeted enforcement and built cases for prosecution, presented and testified for cases at the state and federal level, wrote and executed warrants, and wrote after-action reports.

4. On January 13, 2020, I began my second detail at Tucson Sector Prosecution Unit as a case agent. As a case agent, I conduct investigations involving illicit activity and gather and structure evidence and facts pertaining to administrative and criminal cases. I take sworn statements from material witnesses and suspects. I routinely perform record checks through various law enforcement databases to establish accuracy of information as well as to gather facts relevant to cases. I am a liaison between the United States Attorney's Office and field agents, and I have assisted fellow agents in the development of their cases.

5. Through my training and experience with Alien Smuggling Organizations ("ASOs"), I have learned that the utilization of cellular phones to communicate between coordinators, foot guides, load drivers, stash house operators, etc., is the most common form of communication. Cellular phones often contain evidence that reveals or suggests who possessed or used the device; evidence of where such persons were when they possessed or used the device; evidence of who such persons were with when they possessed or used the device; evidence of persons with whom they communicated when they possessed or used the device; evidence of text, email, other electronic messaging applications, and voice mail communications between the person who possessed or used the device and others. It is quite common for navigational coordinates to also be transmitted to and/or from these devices to determine the user's location through a GPS application. In many areas of the border, scouts use cellular phones to guide the groups to the pickup

locations. Drivers of scout vehicles are able to relay information to the driver of the load vehicle either with a direct call or with applications ("apps") such as WhatsApp. Scouts will relay information such as the presence of Border Patrol. Drivers can also be guided by "pin drops" on apps such as Google Maps which will contain directions for the load vehicle. ASOs will utilize several different apps and functions on their phones to facilitate the coordination of a smuggling event, all the way from inception of the alien to delivery of the alien at the desired location in the United States. In addition, the apps that ASOs use may vary from cellular phone to cellular phone.

6. The statements contained in this affidavit are based on information provided by fellow Border Patrol Agents and based on my experience as a Border Patrol Agent. Since this affidavit is submitted for the limited purpose of securing a search warrant, I have not included all facts known to me regarding this investigation. I have set forth facts that establish probable cause to believe that the defendants referred to in this investigation conspired with each other and known and unknown individuals, wherein they jointly facilitated, either verbally or electronically, the movement of illegal aliens into and within the United States. This affidavit is intended to show only that there exists sufficient probable cause for the requested warrant and does not portray all of my knowledge about this matter.

7. I submit this affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the contents of electronic communication devices capable of accessing the internet, defined below as

Target Device 1 (TD-1), and the extraction from **TD-1** of electronically stored information further described in Attachment B.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

8. The property to be searched consists of one cellular phone. The cellular phone to be examined is an LG Cell Phone, bearing IMEI number: 355041618735117, belonging to Henry LOPEZ-Torres, (hereinafter, **TD-1**). **TD-1** is currently stored at the Nogales Border Patrol Station's evidence vault, maintained by the station's Seized Property Specialist. **TD-1** to be searched pursuant to the attached Application are further described in Attachment A.

9. The requested warrant would authorize the forensic examination of **TD-1** for the purpose of identifying electronically stored data as described in Attachment B.

PROBABLE CAUSE

10. On September 27, 2021, Border Patrol Agents assigned to the Nogales Border Patrol Station's Interstate 19 checkpoint in Amado, Arizona encountered a 2006 Jeep Commander with two male occupants. Agents identified the driver as Henry LOPEZ-Torres and the passenger as Angel Ortega-Movua.

11. At primary inspection, agents questioned the occupants as to their citizenship. LOPEZ-Torres told agents that he was a United States citizen and so was Ortega-Movua. In attempts to distract agents, LOPEZ-Torres tried handing agents birth certificates while they tried to question Ortega-Movua about his citizenship.

12. Agents noticed that Ortega-Movua was very nervous and was avoiding eye contact with agents. Agents asked Ortega-Movua where they were headed, but he appeared

hesitant to answer the question. Agents asked Ortega-Movua for other forms of identification but claimed to only have the birth certificate that LOPEZ-Torres handed to them.

13. Agents referred the vehicle to secondary inspection to further conduct their immigration inspection. Once at secondary, agents obtained consent for fingerprints identification from Ortega-Movua. Agents advised Ortega-Movua that the name displayed on the birth certificate did not match that name from his fingerprints record check. At that time, Ortega-Movua admitted to his true name and to being a citizen of Mexico illegally present in the United States. At that time, both subjects were arrested and transported to the Nogales Border Patrol Station for processing.

14. On October 22, 2021, a video deposition was conducted where Ortega-Movua testified about his arrangements to enter the United States illegally, his travel through the desert, being picked up on the side of a road and taken to a hotel in Nogales, Arizona, where he met a female coordinator "Mariana", LOPEZ-Torres, and another individual. Mariana gave Ortega-Movua the birth certificate to memorize in case he was questioned by immigration officials. LOPEZ-Torres and Ortega-Movua shared a room for the night and the next day traveled north towards Phoenix, Arizona. LOPEZ-Torres told Ortega-Movua to claim they were cousins if they were questioned at the checkpoint. LOPEZ-Torres used a cellphone during the drive north and Ortega-Movua could hear him

and Mariana talking during the calls. LOPEZ-Torres was giving Mariana updates that everything was going fine. They were apprehended at the immigration checkpoint.[1]

15. Based on these facts, I believe that **TD-1**, which was seized during the arrest of LOPEZ-Torres, was used to communicate with members of the Alien Smuggling Organization prior to and during the smuggling venture in order to facilitate the crime of guiding and transporting illegal aliens for profit.

16. Since the date of the arrest, **TD-1** has been stored in the Sonoita Border Patrol Station vault, maintained by the Sonoita Station Seized Property Specialists and transferred to the Tucson Sector Prosecutions Unit's evidence safe, maintained by the Tucson Sector Prosecutions management team.. **TD-1** has been stored in such a manner that its contents, to the best of my knowledge, are in substantially the same state as when they first came into possession of the USBP.

/ / /

[1] During cross-examination, Ortega-Movua admitted he had not been truthful with Border Patrol agents during his post-apprehension interview on the specific issue of when he had first met LOPEZ-Torres during the smuggling event. During the video deposition, he testified that he had met LOPEZ-Torres at the hotel. He explained that in his Border Patrol interview he had claimed to have met him for the first time when LOPEZ-Torres picked him up the next morning. Ortega-Movua stated he was scared at the time of the initial interview because the smugglers had his phone and identification, and he was concerned about what would happen to him if he was immediately returned to Nogales, Mexico by Border Patrol. When the defense asked him whether he had told Border Patrol agents about Lopez-Torres speaking to Mariana on the phone, Ortega-Movua explained that agents had asked him different questions during their interview and the phone calls on the drive to the checkpoint had not come up in their questions.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) Wireless telephone: A wireless telephone (or mobile telephone or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b) Digital camera: A digital camera is a camera that records pictures and video as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded

images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos. Most cell phones currently manufactured contain digital cameras as a standard feature.

c) Portable media player. A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock or games. Most cell phones currently manufactured contain portable medial players as a standard feature.

d) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state. Most cell phones currently manufactured allow the use of the Internet as a

standard feature. Further, most current cell phones allow the user to transmit electronic messages via standard email services or specially designed communication applications between parties.

20. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device; evidence of where such persons were when they possessed or used the device; evidence of who such persons were with when they possessed or used the device; evidence of persons with whom they communicated when they possessed or used the device; evidence of text, email, other electronic messaging applications and voice mail communications between the person who possessed or used the device and others. Navigational coordinates may also be transmitted to and/or from these devices to determine the user's location through a GPS application.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training and experience, I know that electronic devices such as **TD-1** in this case, can store information for long periods of time. Similarly, things that have been viewed via or uploaded to the Internet are typically stored for some period of time on the device. Additionally, computer files or remnants of such files can be recovered even if they have been deleted. This is because when a person "deletes" the information on an electronic device, the data does not actually disappear, rather, the data remains on the storage medium until it is overwritten by new data. Information described

in this affidavit can often be recovered by forensic computer experts using forensic tools and software.

22. As further described in this affidavit and Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how **TD-1** was used, where it was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on **TD-1** as more fully set forth in the factual section contained herein and because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file, including frequency channels, text messages, video, or photographs.

B. Forensic evidence on a device can also indicate who has used or controlled the devices. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

C. A person with appropriate familiarity of how an electronic device works may, after examining the forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a

computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, when and where, sometimes it is necessary to establish that a particular thing is not present on a storage medium, for example, the absence of the entry of a name in a contact list as evidence that the user(s) of device did not have a relationship with the party.

23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of **TD-1** consistent with the warrant. The examination may require authorities to employ techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of **TD-1** to human inspection in order to determine whether it is evidence described by the warrant.

24. If **TD-1** is damaged beyond repair, password protected or otherwise inoperable, less invasive data analysis techniques will not accomplish the forensic goals of the examination. If this is true, an analysis technique referred to as "chip off" may be implemented to conduct the data extraction process. Chip-off is an advanced digital data extraction and analysis technique that would involve physically removing flash memory chip(s) from **TD-1** and then acquiring the raw data using specialized equipment. This process would render **TD-1** unusable.

25. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. Based on the foregoing information, there is probable cause to believe that **TD-1** contains evidence related to violations of 8 U.S.C. § 1324. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of **TD-1** described in Attachment A to seek the items described in Attachment B.

ADRIAN GOMEZ

Digitally signed by ADRIAN GOMEZ
Date: 2021.11.05 11:40:22 -07'00'

Adrian Gomez, Border Patrol Agent
United States Border Patrol

Subscribed and sworn to before me telephonically
this 5th day of November, 2021:

Honorable Eric J. Markovich
United States Magistrate Judge
District of Arizona